INDEPENDENT SECTOR

Updated 5/31/24

The American Privacy Rights Act (APRA)
Summary and Issues for Nonprofits

On April 7, 2024, House Energy & Commerce Committee Chairman Cathy McMorris Rodgers (R-WA) and Senate Commerce Committee Chairman Maria Cantwell (D-WA), released a discussion draft of the American Privacy Rights Act (APRA) that would provide new and tougher privacy rights governing the collection and use of consumer data. That discussion draft was later updated and advanced by a key subcommittee on May 23, 2024. The bill's new enforceable federal standard seeks to eliminate the patchwork of state privacy laws, building on much of the language in the 2022 American Data Privacy and Protection Act (ADPPA). The 2022 bill was a product of negotiations among McMorris Rodgers, House E&C Ranking Member Frank Pallone (D-NJ) and then-Senate Commerce Committee Ranking Member Roger Wicker (R-MS) and was overwhelmingly approved by the House Energy & Commerce Committee in 2022 but was never voted on by the full House and was not reintroduced.

Unlike the 2022 bill, the initial version of APRA did not include the same strong language on children's data. This raised concerns for some legislators, which partially explains why a child-focused privacy bill was added to APRA in May, 2024.

Language on Nonprofits

Nonprofits are specifically included within the bill's ambit: Under the draft, the bill's rules on handling data would apply to "covered entities." The draft defines a covered entity as "any entity that, alone or jointly with others, determines the purposes and means of collecting, processing, retaining, or transferring covered data, and— (I) is subject to the Federal Trade Commission Act; (II) is a common carrier subject to title II of the Communications Act of 1934 as currently enacted or subsequently amended; or (III) *is an organization not organized to carry on business for their own profit or that of their members."*

Inclusion of nonprofits in the APRA expands the impact on nonprofit organizations beyond the current data privacy laws in several states. Traditionally, because the Federal Trade Commission's primary jurisdiction applies to matters "in or affecting commerce," most nonprofit organizations have been considered exempt from FTC consumer protection enforcement. Many comprehensive state-level data privacy laws specifically exempt nonprofits from their requirements, while some contain special rules of applicability for nonprofits.

Carve-out for fraud-focused nonprofits: The APRA definition "includes any entity that controls, is controlled by, is under common control with, or shares common branding with another covered entity," but does not include, "except with respect to the obligations under section 9, *a nonprofit organization whose primary mission is to prevent, investigate, or deter fraud or to train anti-fraud professionals or educate the public about fraud,* including insurance fraud, securities fraud, and financial fraud to the extent the organization collects, processes, retains, or transfers covered data in furtherance of such primary mission."

FTC is specifically authorized to enforce against nonprofits: In section 117, which outlines the enforcement authority of the FTC, the bill says that violations of APRA, or any regulation promulgated under APRA, "will be treated as a violation of a rule defining an unfair or deceptive act or practice as prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act." This section reiterates that the Commission will enforce APRA and its regulations as violations of FTC rules prohibiting unfair or deceptive acts specifically "with respect to... *organizations not organized to carry on business for their own profit or that of their members."*

Small-business exemption and nonprofit revenue: The bill exempts "small businesses" from its requirements, with a small business defined as "an entity (including any affiliate of the entity):

- "whose average annual gross revenues for the period of the three preceding calendar years (or for the period during which the covered entity has been in existence if such period is less than three years) did not exceed $40 million, with future updates to this threshold based on SBA size standards;
- "that, on average, did not annually collect, process, retain, or transfer the covered data of more than 200,000 individuals for any purpose other than initiating, rendering, billing for, finalizing, completing or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return or warranty policy; and
- "that did not transfer covered data to a third party in exchange for revenue or anything of value."

Given the annual gross revenues cap in order to be considered a small business, the bill creates **a special definition of "revenue" for nonprofits:** "The term 'revenue,' as it relates to any entity that is not organized to carry on business for its own profit or that of their members, means the *gross receipts the entity received in whatever form from all sources without subtracting any costs or expenses, and includes contributions, gifts, non-Federal grants, dues or other assessments, income from investments, or proceeds from the sale of real or personal property.*"

Transfer between affiliates or federated nonprofit organizations: Unlike the initial discussion draft, the May draft exempts transfers of data between nonprofit entities that are part of the same federated nonprofit organization from the definition of a "third party" transfer. The bill defines a "federated nonprofit organization" as a network of 501(c)(3) organizations that share common branding. As a result, transfers of data between a nonprofit network's national office and a separately controlled affiliate may be exempt from the requirements of other transfers under the bill.

Heightened Requirements for Three Special Categories of Organization

The bill defines three special categories that must meet the toughest rules: 1) large data holders, 2) data brokers, and 3) covered high-impact social media companies.

- Under the bill, a **"large data holder"** is a covered entity or service provider that in the most recent calendar year (1) had an annual gross revenue of $250,000,000 and (2) collected, processed, retained or transferred either the (a) covered data of more than 5,000,000 individuals, 15,000,000 portable connected devices, and 35,000,000 connected devices, or (b) the sensitive covered data of more than 200,000 individuals, 300,000 portable connected devices, and 700,000 connected devices. Certain data points would be excluded, though; an entity would not be considered a large data holder if it only collects personal mailing addresses, email addresses or phone numbers.

- A **data broker** is defined as a "covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to such covered data."

- A **"covered high-impact social media company"** is defined as "a covered entity that provides any internet-accessible platform where – (A) such covered entity generates $3 billion or more in global annual revenue, including the revenue generated by any affiliate of such covered entity; (B) such platform has 300 million or more global monthly active users for not fewer than three of the preceding 12 months; and (C) such platform constitutes an online product or service that is primarily used by individuals to access or share user-generated content."

Minimizing Data

Some analysts have said the bill's data minimization provisions are its most consequential element. APRA says covered entities must not "collect, process, retain, or transfer covered data of an individual beyond what is necessary, proportionate and limited" to provide specific goods and services, or to send reasonably anticipated communications, or for one of 15 expressly permitted purposes. APRA's "necessary, proportionate and limited" standard appears more restrictive than the standard used in the 2022 ADPPA, which limited data processing to "what is reasonably necessary and proportionate."

16 'Permitted Purposes' for Data Processing. The draft would specifically allow data processing for the following permitted functions:

1. Protecting data security;
2. Complying with legal obligations;
3. Making legal claims;
4. Transfers to law enforcement pursuant to a warrant, administrative subpoena, or other lawful process;
5. Effectuating a product recall or fulfilling a warranty;
6. Conducting market research (which requires affirmative express consent for consumer participation);
7. With respect to data already lawfully collected under APRA, de-identifying data for use in product improvement and research;
8. Asset transfers in mergers and acquisitions;
9. Telecom and mobile carriers providing call location information for emergency services;
10. Preventing fraud and harassment (though not for selling to government agencies, including law enforcement);
11. Responding to an ongoing or imminent network security or physical security incident;
12. Responding to ongoing or imminent security incidents or public safety incidents (though not for selling to government agencies, including law enforcement);
13. Responding to criminal activity (though not for selling to government agencies, including law enforcement, and not health information);

14. Processing non-sensitive data for first party of contextual advertising; and
15. Processing non-sensitive data for targeted advertising
16. Conducting peer-reviewed science in the public interest.

Notably, in what some described as "post-Dobbs" language, purpose #13 forbids the collection of health data to respond to criminal activity.

Other Major Requirements for Covered Entities

Transparency: The draft requires covered entities and their service providers to make available, "in a clear, conspicuous, not misleading, easy-to-read manner," a privacy policy that accurately details its data collection, processing, retention, and transfer activities.

Executive responsibility: The bill outlines two layers of executive responsibility requirements: 1) baseline requirements for all covered entities and service providers, and 2) heightened requirements for large data holders. Large data holders would have to make certifications to the FTC and submit privacy impact assessments.

Incident response requirements: Under the new bill, both covered entities and service providers must "establish, implement, and maintain reasonable data security practice,." such as vulnerability assessments, preventative and corrective actions, and training.

Privacy by design: The May 2024 draft adds a new section requiring covered entities and service providers to develop data privacy policies that consider various factors, including the nature of their activities, the sensitivity and volume of data they collect, the cost of implementing controls, and whether the covered entity is a nonprofit. The Federal Trade Commission is directed to issue guidance around what constitutes a reasonable policy within 1 year of enactment, and is directed to "consider unique circumstances applicable to nonprofit organizations**"** and other covered entities.

Enforcement - Role of the FTC

Notably, the bill tasks the Federal Trade Commission (FTC) with providing "guidance" on what is "reasonably necessary and proportionate" to comply with the bill's data minimization requirements. Organizations looking to innovate new ways to use consumer data that aren't covered under the 16 permitted purposes would have to make such a case to the FTC, but guidance in this case falls short of actual rulemaking authority, and some analysts have said that truly new "permitted purposes" may have to be established by legislation.

The bill directs the FTC to "establish within the Commission a new bureau comparable in structure, size, organization, and authority to the existing bureaus within the Commission related to consumer protection and competition," to help the FTC exercise its authority under APRA. The new bureau must be "established, staffed and fully operational not later than one year after the date of enactment of this Act."

State enforcement: State attorneys general, the chief consumer protection officer of a State, or an officer or office of a State authorized to enforce privacy or data security would be able to seek a range of

relief for violations of APRA, including injunctive relief, civil penalties, restitution, and other appropriate relief.

Private Right of Action

The APRA would establish what looks to be a broad and complex private right of action for consumers who allege violations of the law. While the law's default remedy is actual damages, injunctive relief, and attorney's fees, in some instances, the consumer may seek statutory damages. The bill contemplates an opportunity for the covered entity to cure prior to lawsuits in some circumstances. The bill would also prohibit arbitration agreements as to claims alleging violations of the privacy law that involve a minor or that result in a substantial privacy harm. The bill specifically allows residents of California to recover statutory damages consistent with the California Privacy Rights Act for an action related to a data breach.

Pre-emption of State Privacy Laws

The question of whether and how to pre-empt existing state privacy laws like the California Consumer Privacy Act (CCPA) was among the principal reasons the 2022 ADPPA never made it to the House floor, as then-Speaker Nancy Pelosi (D-CA) and much of the California House delegation opposed that bill's pre-emption language. Republicans, however, are unlikely to accept any data privacy bill that allows such laws to remain on the books. Perhaps with that in mind, the APRA discussion draft is carefully worded on this issue: it would generally pre-empt state laws that are covered by the APRA, but it lists various state laws that would not be pre-empted, including state breach notification laws; laws that address employee privacy; and laws that address health information privacy. The draft presents a long list of exceptions, which, according to the law firm Wiley Rein, "makes the exercise of determining which laws are pre-empted and which laws are not a complicated one."

The draft indicates that while state laws would largely be pre-empted, APRA also would empower the same enforcers of those laws to instead enforce the APRA, including attorneys general as well as any "officer or office of the State authorized to enforce privacy or data security laws applicable to covered entities or service providers."

Consumer Rights Established by APRA

The bill would establish rights that already exist under some state privacy laws, including the following rights, which are subject to verifiable requests and all relate to covered data about a specific individual:

- The right to access covered data;
- The right to correct inaccurate or incomplete covered data;
- The right to delete covered data; and
- The right to export covered data.

The bill also would establish the right to opt out of certain processing – specifically the right to opt out of covered data transfers and the right to opt out of targeted advertising.

While these rights are broadly comparable to most state privacy laws, there are some notable differences. Under the right to access, APRA would give individuals the right to access the specific name of any third party or service provider to whom covered data has been transferred and the purpose of

the transfer. That language goes beyond any comprehensive state privacy law enacted to date, including Oregon's new law.

Outlook - Factors to Consider

Chairman McMorris Rodgers has announced that she will be retiring at the end of this Congress and likely views APRA as a "legacy bill". The full Energy and Commerce Committee could mark up and pass the updated version of this bill as soon as June. However, with a dwindling legislative calendar and potential jurisdictional claims by other committees, there may not be enough time for Congress to process this wide-ranging bill. The question will quickly become whether the new approach could secure 60 votes in the Senate or the two-thirds House supermajority necessary to pass a bill under suspension of the rules, given the difficulty of the House GOP leadership to process partisan Rules to govern floor debate for bills with such a small majority in the House.

AI - As artificial intelligence (AI) emerges more into the policy spotlight, many lawmakers have come to believe that the absence of a federal data privacy law is hindering their ability to address some AI concerns. McMorris Rodgers has stressed the need for a national data privacy standard as a "first step towards a safe and prosperous AI future." Toward that end, the draft includes some rules about algorithms that could serve as a starting point for AI regulation in the data privacy framework.

Abortion – In the post-Dobbs era, many Democrats who have campaigned against the Supreme Court's abortion ruling are eager to pass a federal privacy law that addresses issues they say are now raised by consumer health apps and other health and tracking technologies.

Litigation - Republican members who oppose excessive trial lawyer suits will likely be critical of the bill's language establishing a private right of action to address data privacy violations, which one conservative foundation called "the most expensive part of the bill."